Supplement to the Key Bridge Proposals to Administer a Spectrum Access System and a Environmental Sensing Capability

Response to FCC Request for Supplemental Information

GN Docket No. 15-319

Key Bridge LLC

Jesse Caulfield, CEO

1750 Tysons Blvd., Suite 1500
McLean, VA 22102

Phone: +1 (703) 542-4140

http://keybridgewireless.com

Document Information

Document Status	Public
Version	1.0.0
Date Printed	September 27, 2016
Copyright	

Opening Letter

Key Bridge LLC (fmr Key Bridge Global LLC, dba “Key Bridge”, “Key Bridge Wireless”) is pleased to submit this supplement to our proposals to administer a Spectrum Access System (SAS) and a Environmental Sensing capability (ESC) in the 3.5 GHz frequency band.

This document is written to be directly responsive to the questions posed and, accordingly, makes reference to our separate *Proposal to Administer a Environmental Sensing Capability* and to our *Proposal to Administer a Environmental Sensing Capability*.

We thank the Commission for this opportunity and are happy to provide any additional information the Commission may require to evaluate our proposals.

/s/

Jesse Caulfield, CEO
Key Bridge LLC

Response to Request for Supplemental Information

Below we directly respond to each item in the Commission's letter requesting supplemental information, received September 02, 2016.

1. WTB/OET recently released a Public Notice establishing the final methodology for determining Grandfathered Wireless Protection Zones. 9 Please update your proposal to describe how your SAS will protect Grandfathered Wireless Broadband Licensees accordingly. (SAS proposal pg. 66) (§ 96.63(m)) 10	Reference SAS Proposal Section 6.6.1 (Protecting Grandfathered Wireless Broadband Licensees) (below) The Key Bridge SAS strategy to protect Grandfathered Wireless Broadband Licensees is described in the proposal supplement Section 6.6.1 below. The method of procedure is detailed in the attached document *CBRS MOP - Protecting Grandfathered Wireless Services*.
2. Please describe in detail the methods that will be used to update software and firmware for ESC sensors and decision functions. (SAS proposal pg. 103, ESC proposal pg. 67) (SAS / ESC Proposal PN)	Reference ESC Proposal Section 7.3.1 (Software and Firmware Update Security) (below) The Key Bridge ESC strategy to cryptographically secure software and firmware is described in Section 7.3 of our ESC Proposal and clarified in Section 7.3.1 of this supplement (below).
3. Please describe in detail the specific ESC sensing architecture to be deployed and describe how functions will be split between the SAS and ESC. (pgs. 25-26) (SAS / ESC Proposal PN)	Reference ESC Proposal Section 6.2 (Logical Partitioning Strategy), Section 6.3 (Geographic Partitioning Strategy) and Section 6.5 (Direct Sensing Methodology) In the Key Bridge ESC Proposal we describe a common physical infrastructure and two possible methods to detect non-informing incumbent users. The Key Bridge ESC will implement the Direct Sensing Methodology of non-informing incumbent users as described in Section 6.5 of our ESC Proposal.
4. What is the relationship between the proprietary SAS Gateway Protocol and the "various open-source implementation examples" that Keybridge discusses in its proposal? *Please describe in detail whether Keybridge plans to use*	Reference SAS Proposal Section 7.3.2 (SAS to SAS Peering) The Key Bridge SAS implements two message exchange protocols, the use of which is determined by the scope of operation: Internally, between systems under Key Bridge control; and Externally, between different autonomous systems.

proprietary/non-proprietary and/or standardized/non-standardized solutions. (pg. 95) (§ 96.53)	Internally the Key Bridge SAS Nodes will use a proprietary intra-SAS Node messaging protocol. Key Bridge will share details of this protocol with the FCC and other responsible parties to facilitate SAS evaluation, testing and certifyication. Externally the Key Bridge SAS will communicate with other FCC-authorized SAS instances via a mutually-agreed inter-SAS peering protocol. The present candidate protocol, developed through a multi-stakeholder group, is the Wireless Innovation Forum's *SAS-to-SAS Peering Protocol*.
5. Please describe in detail how Keybridge will receive and addresses reports of interference and requests for additional protection from incumbent access users and promptly address these reports of interference. (pg. 74) (§ 96.53(o))	Reference SAS Proposal Section 6.10.2 (Interference Incident Reporting and Resolution), Section 11 (Appendix: SSRF Interference Incident Report), and Section 12 (Appendix: Joint Spectrum Interference Resolution) Also reference Section 13 (Appendix: Endorsement of Standard Spectrum Resource Format Version 3.x) (below) The Key Bridge SAS will implement a commercial, CBRS-compliant version of the JSIR process using the OpenSSRF implementation of the SSRF v3.1 protocol.[1] These two standards form the basis for DOD existing interference incident reporting and resolution procedures and information systems. The SSRF protocol is formally endorsed by the Wireless Innovation Forum.[2] OpenSSRF, a software implementation of the SSRF protocol, was sponsored by the Wireless Innovation Forum and developed by Key Bridge in collaboration with other members and the Defense Spectrum Organization. OpenSSRF is an officially recognized reference implementation of the SSRF v3.1 standard.[3]

1 See OpenSSRF Reference Implementation at http://openssrf.org

2 See Wireless Innovation Forum Working Document WINNF-14-R-0019, Version V1.0.0, January 12, 2015 (attached)

3 See Defense Information Systems Agency Letter to Jesse Caulfield, CEO, Key Bridge, August 07, 2015 (attached)

6. Please discuss specifically how the SAS will protect existing FSS earth stations and comply with each subsection of FCC rule section 96.17. The Keybridge proposal refers to "ongoing discussions in multi-stake holder group" on FSS protection. Please include updates based on such developments and if/where your approach is different from such procedures. If the SAS will permit excessive CBSD emissions upon mutual agreement, please discuss how the SAS will obtain the terms of this agreement and how it will communicate the terms promptly to other SAS Administrators. (pg. 64) (§ 96.17)	Reference SAS Proposal Section 6.6.2 (Protecting Existing Fixed Satellite Service Earth Stations) (below) The Key Bridge SAS strategy to protect FSS earth stations is described in the proposal supplement Section 6.6.2 below. The method of procedure is detailed in the attached document *CBRS MOP - Protecting FSS Earth Stations*.
7. Please describe in detail the methods used to ensure secure SAS-ESC communications and your security protocols, including whether this includes proprietary solutions. (pg. 91) (SAS / ESC Proposal PN)	Reference ESC Proposal Section 7.2 (Communications Security) Key Bridge will ensure all communications and interactions between the the Key Bridge ESC and a peering SAS are accurate and secure and that unauthorized parties cannot access or the information the ESC sends to a SAS, consistent with 47 CFR §96.61(b). The Key Bridge ESC employs several industry standard, non-proprietary and widely adopted technologies and strategies to ensure communications security. These include: • Network firewall filters to ensure only authorized hosts may connect to ESC services • Mutual, counter-party authentication using X.509 digital certificates and public/private key pairs • Enforcement of transport layer security for all communication sessions • End-to-end message validation, authentication and non-repudiation

	The Key Bridge ESC to SAS peering strategy is based upon open, widely adopted, non-proprietary standards, technologies and systems.
8. Please describe in detail how the SAS will address adjacent channel and blocking issues caused by nearby CBSDs. (§§ 96.17(a)(2), (3))	Reference SAS Proposal Section 6.6.2 (Protecting Existing Fixed Satellite Service Earth Stations) (below) and the attached document *CBRS MOP - Protecting FSS Earth Stations*. Candidate CBSDs that may require SAS interference mediation are identified based upon their proximity to a protected FSS earth station. The calculating methodology for the specific FSS-received interference power level of each candidate CBSD includes a frequency dependent rejection (FDR) parameter. FDR is a measure of the frequency rejection produced by the receiver on unwanted transmitter emissions. The FDR component of the FSS-received interference power level equation accounts for CBSD co-channel vs. adjacent channel determination and blocking.
9. Please provide a detailed description of the SAS-ESC communication protocol and the parameters which are exchanged between the ESC and SAS, including what information will be exchanged between the ESC function and the SAS function. As a combined SAS-ESC applicant, Keybridge should explain in detail the testing interfaces to demonstrate how these communications and data transmissions can be conducted securely. (pg. 91) (SAS / ESC Proposal PN)	The Key Bridge SAS-to-ESC Peering Protocol is presently under active development by Key Bridge and other collaborating partners. Once finished, Key Bridge plans to publish the protocol and make it available for use by others without constraint. We respectfully request two additional weeks to complete this needed development work.
10. Although Keybridge indicates that it plans to offer leasing, it does not discuss how the SAS will:	The Key Bridge Spectrum Leasing Implementation Strategy is presently under active development by Key Bridge and other collaborating partners. Once finished, Key Bridge plans to publish the strategy and make it available for use by others without constraint.

	We respectfully request two additional weeks to complete this needed development work.
11. What specific propagation models will Keybridge use to determine power levels? *Please provide a detailed description of such models, including equations, terrain/clutter inputs, etc., for the calculation of aggregate interference to protect incumbents and PALs.*	Reference SAS Proposal Section 6.6.1 and 6.6.2 (below) and the detailed method of procedure documents *CBRS MOP - Protecting FSS Earth Stations* and *CBRS MOP - Protecting Grandfathered Wireless Services.* The Key Bridge SAS will implement and use the ITU Recommendation P.2001-2 model for radiowave propagation loss.[4] The ITU-R P.2001 model is dependent upon an external raster terrain elevation model. The Key Bridge SAS will employ bare-earth elevation raster libraries from the United States Geological Survey National Elevation Dataset (NED) as 1/3, 1 and 2 arc-seconds resolution, depending upon the region of coverage. The ITU-R P.2001 model also includes dependencies on empirically measured meteorological and land cover data. Reference files for these other raster coverages (i.e. all but terrain elevation) are available through the ITU.[5]
In addition, please provide the model Keybridge will use to calculate PAL protection areas. (pgs. 83-96) (§ 96.53(c))	A model to calculate consistent PAL protection areas across different SASs is presently under development within the Wireless Innovation Forum, a multi-stakeholder group, in which Key Bridge is an active participant. Present issues under discussion include whether and how best to accommodate contour islands, holes, spikes, incursions and other artifacts introduced from terrain effects in radial path loss estimation. Key Bridge is an active participant in this effort and intends to implement the common, rules-compliant PAL protection area model developed through the Wireless Innovation Forum.

4 See P.2001 : A general purpose wide-range terrestrial propagation model in the frequency range 30 MHz to 50 GHz (2015) (available through agency at https://www.itu.int)

5 Ibid.

12. Please provide additional details and updates regarding Keybridge's proposed SAS-SAS peering model to demonstrate that it will make necessary information available to other SASs. (pg. 95) (§96.55(a)(2))	Reference response to Question 4 above. Externally the Key Bridge SAS will communicate with other FCC-authorized SAS instances via a mutually-agreed inter-SAS peering protocol. The present candidate protocol, developed through a multi-stakeholder group, is the Wireless Innovation Forum's *SAS-to-SAS Peering Protocol*.

Proposal Supplement

The following sections supplements our *Proposal to Administer a Spectrum Access System* or our *Proposal to Administer a Environmental Sensing Capability*.[6] Each section identifies its associated document and is numbered according to its position in the updated proposal document.

6 See Key Bridge *Proposal to Administer a Spectrum Access System* (SAS Proposal) and *Proposal to Administer a Environmental Sensing Capability* (ESC Proposal), GN Docket 15-319, both submitted March 15, 2016.

The following section supplements our SAS Proposal and is numbered according to its position in the updated document.

6.6.1 Protecting Grandfathered Wireless Broadband Licensees

Coincident with the submission of our proposal to the Commission, the Wireless Telecommunications Bureau released a Public Notice establishing the final methodology for determining and protecting Grandfathered Wireless Broadband Services.[7]

Key Bridge has reviewed this guidance and confirms the Key Bridge SAS will implement the procedure detailed in the Grandfathered Licensee Methodology PN and also previously discussed in the Commission's request for comment.[8]

Key Bridge will implement the calculation of protection zones for Grandfathered Wireless Broadband Services according to the metrics and procedures identified in the Grandfathered Licensee Methodology PN plus currently available information in the ULS database. The Key Bridge SAS implementation strategy to protect grandfathered wireless broadband services is detailed in the attached *CBRS Method of Procedure* document titled "Protecting Grandfathered Wireless Services", which brings together and consolidates direct source and indirect reference material into a single implementation manual.

Key Bridge intends to submit the attached method of procedure to the Wireless Innovation Forum for review, extension and adoption as a multi-stakeholder implementation standard.

7 *Wireless Telecommunications Bureau and Office of Engineering and Technology Announce Methodology for Determining the Protected Contours for Grandfathered 3650-3700 MHz Band Licensees*, DA 16-946, GN Docket No. 12-354, Public Notice, (Grandfathered Licensee Methodology PN).

8 *Wireless Telecommunications Bureau Seeks Comment on an Appropriate Method for Determining the Protected Contours for Grandfathered 3650-3700 MHz Band*, GN Docket No. 12-354, Public Notice, DA 15-1208 (Grandfathered Licensee Comment PN).

The following section supplements our *SAS Proposal* and is numbered according to its position in the updated document.

6.6.2 Protecting Existing Fixed Satellite Service Earth Stations

The Key Bridge SAS will faithfully implements the Commission's requirements to protect FSS earth stations in the 3,600 – 3,700 MHz band and 3,700 – 4,200 MHz band by adjusting CBSD transmit power in a manner consistent with the Commission's Part 96 rules. The Key Bridge SAS will protect existing fixed satellite service earth stations, as required by and described in 47 CFR §96.17, in a manner similar to the sequential process described in the Google Proposal and detailed in the attached *CBRS Method of Procedure* document titled "Protecting FSS Earth Stations".[9]

Key Bridge will implement the calculation of protection zones for Grandfathered Wireless Broadband Services according to the procedures identified in 47 CFR §96.17, §2.106, §25.209(a)(1) and (4), etc. and the most current information available from the FCC. The SAS method of procedure is detailed in the attached *CBRS Method of Procedure* document titled "Protecting FSS Earth Stations", which brings together and consolidates the various relevant direct source and indirect reference materials into a single implementation manual.

Key Bridge intends to submit the attached method of procedure to the Wireless Innovation Forum for review, extension and adoption as a multi-stakeholder implementation standard.

9 See *Application of Google Inc. for Certification to Provide Spectrum Access System and Environmental Sensing Capability Services*, GN Docket No. 15-319 Rcd. 05/16/16 (*Google Proposal*)

The following section supplements our ESC Proposal and is numbered according to its position in the updated proposal document.

7.3.1 Software and Firmware Update Security

ESC Service Node and Sensor Node software and firmware may be updated via remote administration through the ESC Administration Portal by authorized Key Bridge personnel.

The Key Bridge ESC Service and Sensor Nodes are based upon a Java virtual machine plus Linux operating system, conceptually similar to the Google Android stack but optimized for embedded, high-availability, remote operation.

ESC Service and Sensor Node firmware consists of Linux kernel modules and libraries plus Java Archive (JAR) libraries. System software consists of OSGI Java Archive (JAR) modeles.

As described in Section 7.2 of the ESC Proposal, all information transfers between the ESC Administration Portal and ESC Service Nodes and Sensor Nodes is cryptographically protected using industry standard communications security practices. Additionally, as described in Section 7.3, all software and firmware components, including operating system kernel modules and libraries, JAR libraries plus OSGI modules, are cryptographically (i.e. digitally) signed.

The receiving ESC Service Node or Sensor Node verifies the digital signature of each software and firmware module upon receipt and prior to loading. Any module failing the security check is rejected and a security-related alert is forwarded to the Key Bridge ESC Administration Portal for inspection and remediation.

The following section supplements our SAS Proposal and is numbered according to its position in the updated proposal document.

13 Appendix: Endorsement of Standard Spectrum Resource Format Version 3.x

See Wireless Innovation Forum Working Document WINNF-14-R-0019

Version V1.0.0

12 January 2015